# METHOD AND APPARATUS FOR DATA ENCRYPTION


## Abstract of the Disclosure

A block cipher device for a cryptographically secured digital communication system includes a pair of first stages connected in parallel for receiving an input data block and a control data block. Each first stage defines a respective first data path and includes a sum modulo-two unit for receiving the control data block and the input data block. Each first stage also includes a first nibble swap unit downstream from the sum modulo-two unit. A key scheduler generates a random key data block based upon a received key data block. A pair of second stages is connected in parallel downstream from the first stages and receives the random key data block, the control data block and output signals from the first stages for providing an output data block. Each second stage defines a respective second data path and includes a plurality of modulo units. The block cipher device further includes a bit diffuser connected in both of the first data paths for mixing data therebetween.